# Tema 7: Tecnologias y Servicios de Seguridad en Internet

## 1. Introduccion

Los requisitos en seguridad de la información manejada dentro de una organización han evolucionado sustancialmente en las últimas décadas. Si en un principio la seguridad de la información recaía en medios físicos y administrativos, con la llegada y enorme evolución de los sistemas informáticos ha surgido la necesidad de desarrollar herramientas automáticas para proteger los ficheros y otras informaciones almacenadas en memoria.

Por otro lado el desarrollo en paralelo de los sistemas distribuido y redes de datos ha dado lugar a la aparición de nuevos riesgos de seguridad relativos a la distribución de la información entre los sistemas informáticos y a la necesidad de reforzar o incluso adaptar al nuevo entorno los controles de seguridad de los sistemas individuales.

El objetivo de este trabajo será el análisis de los riesgos de seguridad en la distribución de la información en redes de comunicaciones. Es necesario integrar las funcionalidades propias de la seguridad en las arquitecturas de comunicaciones existentes. Este proceso de integración implicará la implementación de mecanismos y servicios y funciones de seguridad de seguridad que se apoyarán en muchos casos en servicios, mecanismos y funciones ya implementados en la propia arquitectura de comunicaciones. El resultado final será lo que denominaremos **ARQUITECTURA DE SEGURIDAD**.

Para estimar las necesidades de seguridad de una organización y evaluar y elegir los productos y políticas de seguridad en las comunicaciones, el gestor responsable de la seguridad necesita evaluar los siguientes aspectos en la seguridad de la información:

- **ATAQUES A LA SEGURIDAD**: Qué acciones pueden comprometer la seguridad de la información que pertenece a una organización.
- **MECANISMO DE SEGURIDAD**: Qué mecanismos hay que implementar para detectar, prevenir o recuperarse de un ataque a la seguridad de la información.
- **SERVICIOS DE SEGURIDAD**: Qué servicios ofrecer al usuario respecto a la transferencia de información en una red de datos. Los servicios de seguridad tratan de contrarrestar los ataques y para ello hacen uso de los mecanismos de seguridad para proporcionar ese servicio

- **OBJETIVOS DE SEGURIDAD:** Se puede definir una serie de objetivos o requisitos que la arquitectura de seguridad debe garantizar respecto de los datos que manejan las redes de comunicaciones. Los objetivos son los siguientes:
  1. Protección de los datos frente a modificaciones no autorizadas, así como a pérdidas/repeticiones y revelaciones no autorizadas.
  2. Garantía de la correcta identidad del emisor de los datos así como del receptor de los datos.

  Al alcanzar estos objetivos se asegurara que los datos que son transmitidos de un sistema a otro no han sido modificados, revelados, retransmitidos o perdidos en la red sin que el emisor o el pretendido receptor haya sido notificado y sin que las partes que intervienen en el protocolo hayan sido correctamente identificados.

- **AMENAZAS EN UNA RED TELEMATICA:** Estas amenazas modifican el flujo normal de datos entre un origen y un destino, pueden ser interceptación que amenaza contra la confidencialidad, interrupción que amenaza contra la disponibilidad de un recurso, modificación que amenaza contra la integridad de un recurso o fabricación que amenaza contra la autenticidad.

  Una forma útil de clasificar los ataques a la seguridad, es en activas pasivos y ataques activos.

  - **ATAQUES PASIVOS:** Intenta averiguar o hacer uso de información del sistema, pero sin afectar a los recursos del mismo.
    Consisten en escuchas o monitorizaciones de las transmisiones. La meta del oponente es la de obtener la información que está siendo transmitida.

La divulgación del contenido de un mensaje y el análisis de tráfico constituyen dos tipos de ataques pasivos.

* **DIVULGACION DE CONTENIDO**: Un mensaje puede contener información sensible o confidencial y por ello, desearíamos impedir que un oponente averigüe el contenido de esas transmisiones.
* **ANALISIS DE TRAFICO**: Aunque protejamos nuestros mensajes cifrándolos, el oponente aunque no podría extraer la información del mensaje, podría observar el patrón de estos mensajes y podría determinar la localización y la identidad de los computadores que se están comunicando y observar la frecuencia y longitud de los mensajes intercambiados

Estos ataques son muy difíciles de detectar, ya que no suponen una alteración de los datos, normalmente el trafico de mensajes es enviado y recibido de forma aparentemente normal, sin embargo, es factibles impedir con éxito estos ataques mediante el cifrado.

**-ATAQUES ACTIVOS:** Intenta alterar los recursos del sistema o influir en su funcionamiento.

Suponen alguna modificación del flujo de datos o la creación de flujos falsos. Los podemos clasificar en 4 categorías:

* **ENMASCARAMIENTO**: Tiene lugar cuando una entidad pretende ser otra entidad diferente. Un ataque por enmascaramiento normalmente incluye una de las otras formas de ataques activos.
* **RETRANSMISION**: Supone la captura pasiva de unidades de datos y su retransmisión posterior para producir un efecto no autorizado.
* **MODIFICACION DE MENSAJES**: Algún fragmento de un mensaje legítimo se modifica o que el mensaje se retrasa, reordena para producir un efecto no autorizado.
* **DENEGACION DE SERVICIO**: Impide o inhibe el uso normal o gestión de servicios de comunicaciones. Este ataque puede tener un objetivo específico

Los ataques activos presentan características opuestas a las de los ataques pasivos. Es bastante difícil impedir ataques activos de forma absoluta, ya que para hacerlo se requeriría protección física permanente de todos los recursos y todas las rutas de comunicación.

Los servicios de seguridad tratan de detectarlos y recuperarse de cualquier perturbación o retardo ocasionado por ellos.

Debido a que la detección tiene un efecto disuasivo también puede contribuir a la prevención.

Cuando se habla de servicios de seguridad habría que determinar por un lado el conjunto de servicios que contemplen los objetivos de seguridad definidos y, por otro lado que mecanismos son adecuados o cuales se deberían implementar para cada servicio y finalmente donde deberían estar situados en la arquitectura.

## 2. SERVICIOS DE SEGURIDAD

Un **SERVICIO DE SEGURIDAD** es el servicio proporcionado por un nivel de un sistema abierto que garantiza la seguridad de los sistemas abiertos o las transferencias de datos en dichos sistemas.

Estos servicios están divididos en cinco categorías y catorce servicios específicos.

- **AUTENTICACION:** Asegura que las entidades que se comunican son quién reclaman ser. Se define dos servicios de autenticación específicos:

  **-AUTENTICACION DEL ORIGEN DE LOS DATOS:**

  Este servicio se aplica a comunicaciones no orientadas a conexión donde las unidades de datos son independientes y por lo tanto en este caso lo más que se puede garantizar es que el origen de cada unidad de datos corresponde con la indicada en su cabecera.

  Este servicio puede ofrecerse en aplicaciones como el correo electrónico, donde no hay una comunicación previa entre entidades finales.

  Este servicio está asociado con el servicio de integridad de datos no orientado a conexión; no parece muy útil asegurar la identidad del origen de los datos si no se puede garantizar su integridad.

  **-AUTENTICACION DE ENTIDADES PARES:**

  Este servicio se aplica a comunicaciones orientadas a conexión.

  Este servicio asegura la identidad de las dos entidades que se comunican, es decir, se asegura que cada una es quién dice ser. Posteriormente en la fase de transferencia debe garantizar que un intruso no pueda

suplantar a cualquiera de las dos entidades legítimas que se comunican a efectos de transmisiones o recepciones no autorizadas.

- **CONTROL DE ACCESO:** El servicio de control de acceso evita el uso no autorizado de los recursos.
  Este servicio controla quien puede tener acceso a un recurso, bajo qué condiciones puede tener lugar el acceso y que se le permite hacer a aquel que accede a un recurso.

- **CONFIDENCIALIDAD:** Asegura que la información o no va a ser revelada ni va a estar disponible a individuos no autorizados, entidades o procesos.
  Este aspecto tiene especial importancia cuando las redes de comunicaciones que transportan la información presentan puntos vulnerables respecto de la seguridad.
  Se han descrito cuatro versiones de este servicio:

  **-ORIENTADA A CONEXION:** Consiste en la protección de todos los datos de usuario en una comunicación orientada a conexión

  **-NO ORIENTADA A CONEXIÓN:** Consiste en la protección de todos los datos de usuario contenidos en una sola unidad de datos del servicio (UDS) en una comunicación no orientada a conexión

  **-SELECTIVA:** Consiste en la protección de campos específicos de todas las unidades de datos de usuario de una comunicación orientada a conexión o de una sola unidad de datos del servicio (UDS) en una comunicación no orientada a conexión

  **-APLICADA AL ANALISIS DEL TRÁFICO:** Este servicio sirve para la protección de los datos frente a un análisis del tráfico originado por una comunicación entre entidades pares.

- **INTEGRIDAD:** Asegura que datos son recibidos exactamente a como han sido enviados por una entidad autorizada, es decir sin duplicaciones, retransmisiones, modificaciones o inserciones.
  Cuando se detecta una violación en la integridad de los datos el servicio de integridad puede o bien avisar de que se ha producido este hecho o utilizar mecanismos para la recuperación de la perdida de integridad de los datos. Así se han definido las siguientes modalidades del servicio.

  **-ORIENTADA A CONEXIÓN CON MECANISMO DE RECUPERACION:**
  Proporciona la integridad de todas las unidades de datos de usuario de una comunicación orientada a conexión y detecta cualquier modificación, inserción, borrado o retransmisión de cualquier unidad de datos dentro de una secuencia entera de unidad de datos del servicio (UDS) haciendo uso de mecanismos de recuperación de la integridad si fuera necesario.
  El uso de este servicio junto con el servicio de autenticación de entidad par proporciona un alto grado de protección frente a la mayoría de ataques activos.

  **-ORIENTADA A CONEXIÓN SIN MECANISMO DE RECUPERACION:**
  Este servicio sólo detecta las violaciones en la integridad de los datos pero no se articulan mecanismos de recuperación de la integridad.

  **-ORIENTADA A CONEXIÓN SOBRE CAMPOS SELECTIVOS:**
  Este servicio asegura la integridad de campos específicos dentro de las unidades de datos de usuario en una comunicación orientada a una conexión y toma una determinación de si los campos seleccionados han sido modificados, insertados, borrados o retransmitidos.

  **-NO ORIENTADA A CONEXIÓN:**
  Este servicio asegura la integridad de una sola unidad de datos del servicio (UDS) en comunicaciones no orientadas a conexión teniendo alguna forma de detección de la modificación de una UDS.
  Adicionalmente también pueden existir algunos mecanismos que garanticen la detección de retransmisiones

  **-NO ORIENTADA A CONEXIÓN SOBRE CAMPOS SELECTIVOS:**
  Este servicio asegura la integridad de campos específicos dentro de una sola unidad de datos del servicio (UDS) en comunicaciones no orientadas a conexión. Este servicio toma alguna determinación si los campos seleccionados han sido modificados.

- **NO REPUDIO:** Evita que las entidades pares que se comunican puedan denegar el haber participado en parte o en toda la comunicación. Se han definido dos modalidades del servicio:

  **-CON PRUEBA DE ORIGEN:** Este servicio proporciona los mecanismos necesarios para asegurar que el mensaje fue enviado por la entidad especificada.

-CON PRUEBA DE ENTREGA: Este servicio proporciona los mecanismos necesarios para asegurar que el mensaje fue recibido por la entidad especificada

No repudio es más fuerte que autenticación debido a que no repudio tiene validez legal.

# 3. MECANISMOS DE SEGURIDAD

Los servicios de seguridad son implementados utilizando mecanismos de seguridad. Un servicio de seguridad puede utilizar uno o varios mecanismos de seguridad. En la arquitectura de seguridad definida para el modelo ISA se han definido los siguientes mecanismos de seguridad:

•CIFRADO O ENCRIPTACION:

La encriptación es un mecanismo que utiliza la criptografía para transformar las unidades de datos intercambiadas por las entidades pares.

El mecanismo de encriptación contempla dos funciones a realizar sobre las unidades de datos: LA FUNCIÓN DE ENCRIPTADO Y LA FUNCIÓN DE DESENCRIPTADO.

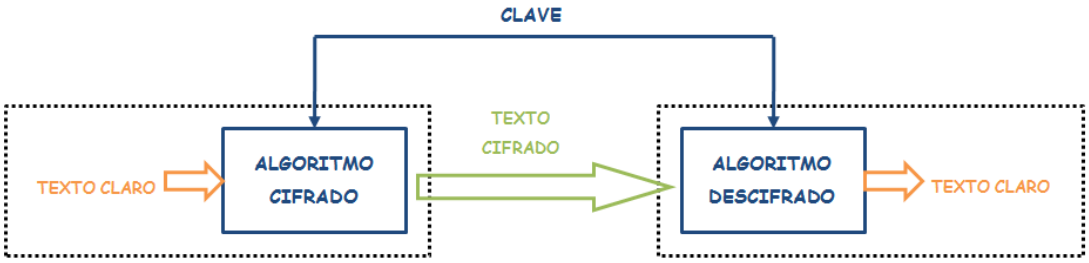
El mecanismo de encriptación protege a los datos de usuario frente a la revelación de los contenidos (estos serán denominados ataques activos).

Antes de realizar la función de encriptado las unidades de datos a intercambiar se denominan TEXTO EN CLARO. Para la transmisión de las unidades de datos una entidad par aplicará la función de encriptado sobre el texto en claro transformándolo a datos ininteligibles, también llamado TEXTO CIFRADO. La entidad receptora de las unidades de datos cifradas deberá realizar la función inversa denominada desencriptado para poder recuperar el texto en claro.

El mecanismo de encriptación se utiliza típicamente para proporcionar el SERVICIO DE CONFIDENCIALIDAD, aunque también puede soportar otros servicios de seguridad como los SERVICIOS DE INTEGRIDAD Y DE AUTENTICACIÓN. Se han definido dos modalidades del mecanismo de encriptado:

-CIFRADO SIMETRICO (CLAVE SECRETA): Las unidades de datos a intercambiar por las entidades pares (texto en claro) se transforman en un texto ininteligible (texto cifrado) al aplicar una función de cifrado.

La función de función tiene dos elementos: el algoritmo de cifrado y una clave que controla dicho algoritmo. El algoritmo de cifrado se aplicará sobre las unidades de datos y obtendrá diferentes resultados al aplicarse sobre las mismas unidades de datos dependiendo de la clave utilizada en cada momento. Cambiando la clave se cambia el texto cifrado obtenido.



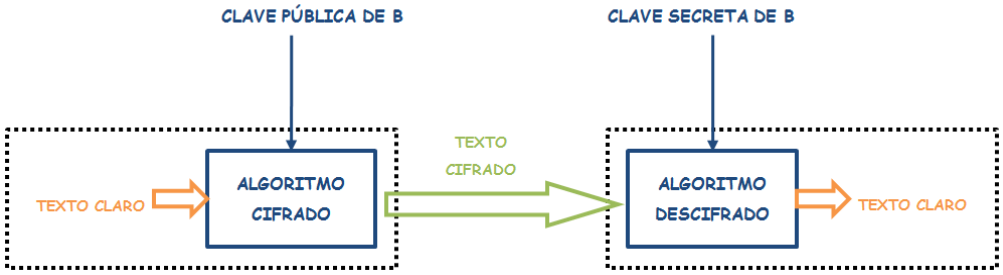

El usuario A genera a partir de un texto en claro un texto cifrado después de aplicar la función de cifrado. El usuario B una vez recibido el texto cifrado puede transformarlo a texto claro usando la función de descifrado. El algoritmo de cifrado y descifrado usan la misma la clave y para ello primero se tendrá que compartir tanto la clave como el algoritmo entre emisor y receptor.

La seguridad del cifrado simétrico depende de varios factores. Primero el algoritmo de cifrado debe ser capaz de hacer inviable desencriptar los datos a partir solo del texto encriptado La seguridad depende del conocimiento de la clave y no del conocimiento del algoritmo de cifrado.

Se tiene que cumplir que:

1. Que la clave sea secreta.
2. Debe ser imposible o impracticable desencriptar un mensaje si no hay otra información disponible.
3. El conocimiento del mensaje cifrado y el algoritmo debe ser insuficiente para conocer la clave.

### -CIFRADO ASIMETRICO (CLAVE PÚBLICA):




En la encriptación de clave pública son esenciales los siguientes pasos:

1. Cada entidad par del sistema final en la red genera un par de claves para ser utilizadas en las funciones de encriptado y desencriptado de datos.
2. Cada entidad par publica su clave de encriptado situándola en un registro público o fichero. Esta es la **CLAVE PUBLICA**. La clave asociada es la **CLAVE PRIVADA.**
3. Si una entidad A desea enviar un mensaje a otra entidad B, encripta el mensaje usando la clave publica de la entidad B.
4. Cuando la entidad B recibe el mensaje, desencripta usando la clave privada de la entidad B. Ninguna otra entidad puede desencriptar el mensaje, ya que sólo la entidad B conoce su clave privada.

Con este modelo todos las participantes tiene acceso a las claves públicas .Las claves privadas son generadas localmente a cada participante y por lo tanto no necesita ser distribuida.
En la medida que un sistema controla su clave privada la comunicación es segura.
En cualquier momento un sistema puede cambiar su clave privada y publicar la clave pública asociada para reemplazar su vieja clave pública.
Se tiene que cumplir que:

1. Que luna de las claves permanezca secreta.
2. Debe ser imposible o inviable desencriptar un mensaje si no hay otra información disponible.
3. El conocimiento del mensaje cifrado y el algoritmo debe ser insuficiente para conocer la otra clave del par.

La generación, distribución y almacenamiento de las claves criptográficas usadas en la encriptación convencional o de clave pública implicaría en la mayoría de los casos un intercambio de información de control entre entidades pares. A estos procedimientos los denominaremos **PROTOCOLOS DE DISTRIBUCION DE CLAVES** o **PROTOCOLOS DE SEGURIDAD**.

## •INTERCAMBIO DE AUTENTICACION:

La autenticación de unidades de datos es un mecanismo que permite que las partes que se comunican verifiquen que los mensajes recibidos son auténticos.
Una unidad de datos, un mensaje, fichero, documento u otra colección de datos se dice que son auténticos cuando son genuinos (no han sido alterados) y vienen de la fuente que alegan venir.
El mecanismo de autenticación protege a las unidades de datos intercambiadas de los denominados ataques activos por parte de los intrusos, es decir de las posibles alteraciones o modificaciones, también se puede desear verificar que las unidades de datos no han sido retardadas artificialmente.
Los mecanismos de autenticación van a implicar el intercambio de una serie de información de control entre las entidades pares implicadas constituyendo un auténtico protocolo, el denominado **PROTOCOLO DE AUTENTICACIÓN.**
Se pueden considerar dos funciones implicadas en los mecanismos de autenticación: el denominado código de autenticación de mensajes y la encriptación.

### -CODIGO DE AUTENTICACION DE MENSAJES:

Esta técnica de autenticación supone el uso de una clave secreta para generar un pequeño bloque de datos conocido como código de autenticación de mensajes y que se incorpora al propio mensaje.

Esta técnica supone que dos entidades que se comunican comparten una clave secreta común $K_{AB}$. Cuando A tiene un mensaje que enviar a B, calcula el código de autenticación del mensaje como función del mensaje y la clave. Luego se transmite el mensaje y el código al destino.
El receptor realiza los mismos cálculos en el mensaje recibido, utilizando la misma clave secreta, para generar el nuevo código de autenticación.
El código recibido se compara con el código calculado. Si asumimos que sólo el receptor y el emisor conocen la identidad de la clave secreta y el código recibido coincide con el código calculado.

Se pueden usar un gran número de algoritmos para generar el código de autenticación. Téngase en cuenta que el mecanismo de código de autenticación es similar a la encriptación. Sin embargo una diferencia clara es que el algoritmo de autenticación no necesita ser reversible como debe ser para la desencriptación. Ello es debido a que las propiedades matemáticas de la función de autenticación es menos vulnerable a ser roto que la encriptación.

**-ENCRIPTACION:**

La encriptación se puede convertir en un mecanismo de autenticación. Así en un modelo de encriptación convencional donde sólo las entidades emisora y receptora comparten la clave secreta únicamente la auténtica entidad emisora podría encriptar con éxito una unidad de datos dirigida a otra entidad. Si además las unidades de datos intercambiadas incluyen un código de detección de errores y un número de secuencia la entidad receptora estará segura de que no se han producido alteraciones y que el número de secuencia es el adecuado

Un modelo de encriptación de clave pública sin embargo no proporciona siempre un mecanismo de autenticación. Encriptando sólo con la clave pública de la entidad receptora sólo se garantiza la confidencialidad de los datos pero no la autenticidad puesto que cualquiera puede conocer la clave pública de la entidad receptora.

El código de autenticación puede tener sentido en determinadas aplicaciones en las que hay que difundir una unidad de datos a muchos destinos y no es recomendable por motivos de coste realizar múltiples funciones de encriptado. También puede ser suficiente para determinadas aplicaciones en la que no es tan importante la confidencialidad de los datos como que esos datos provengan de una entidad específica.

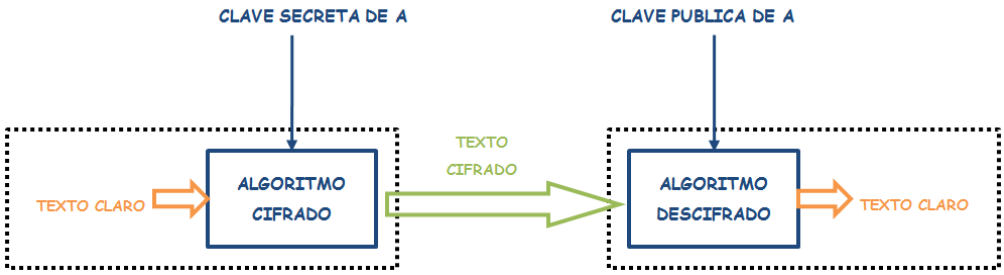
**•FIRMA DIGITAL:**

Puede darse la situación que una entidad receptora podría inventarse una unidad de datos añadir un código de autenticación y decir que viene de la entidad emisora con la que comparte la clave secreta. En estas situaciones es necesario algo más que los mecanismos de autenticación, es por ello que surgen los mecanismos de firma digital. Estos tienen las siguientes propiedades:

1. Debe ser posible verificar al autor, los datos y el tiempo de la firma.
2. Debe ser posible autentificar los contenidos de los mensajes en el tiempo de la firma
3. La firma debe estar disponible por las tres partes para resolver disputas.

La función de firma digital incluye la función de autenticación. Se han definido varias modalidades del mecanismo de firma digital. Así se van a considerar dos categorías denominadas firma digital directa y arbitraria:

**-FIRMA DIGITAL DIRECTA:**




Hay un método de usar la encriptación de clave pública para proporcionar un mecanismo de firma digital la cual incluye autenticación.

Hay que tener en cuenta que los algoritmos de encriptación de clave pública pueden ser empleados en cualquier orden.

La entidad A encripta una unidad de datos con la clave privada de A y se lo manda a la entidad B. La entidad B puede desencriptar el mensaje utilizando la clave pública de A. Puesto que la unidad de datos fue encriptada usando la clave privada de A (y sólo A la conoce) esto quiere decir que la encriptación del mensaje entero sirve de mecanismo de firma digital. Además es imposible alterar la unidad de datos sin acceder a la clave privada de A con lo cual la unidad de datos es a la vez autenticada.

En el modelo anterior la unidad de datos completa es encriptada. Otras opciones serían encriptar una porción mínima de la unidad de datos. Si una porción de la unidad de datos es encriptada con la clave secreta del emisor, sirve como firma que verifica el origen, contenido y secuenciamiento.

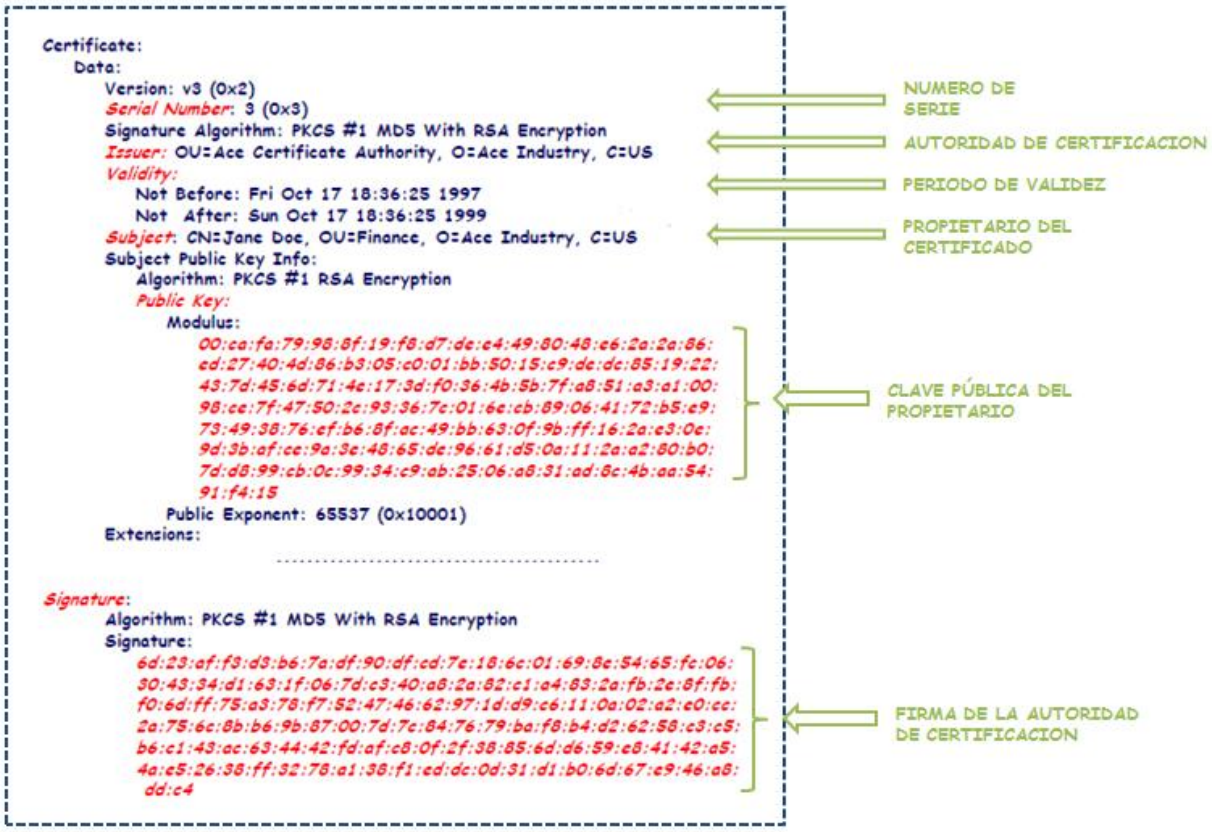
Este modelo sin embargo no garantiza que cualquier intruso no pueda acceder a los contenidos de las unidades de datos.

Esto es obvio en el caso de la encriptación aplicada a una parte de la unidad de datos, ya que el resto de la unidad de datos es transmitido en claro, aunque también ocurre en el caso de la encriptación completa ya que cualquier observador puede desencriptar el mensaje usando la clave pública de la entidad emisora.

## •CERTIFICADO:

Un certificado digital, o certificado de clave publica, establece la identidad de un usuario en una red. Es equivalente a una tarjeta de crédito o a un carnet de identidad.
Un certificado asocia una identidad a una clave pública. Los certificados de seguridad los emiten las **AUTORIDADES DE CERTIFICACIÓN (CA)**.
Una CA utiliza un algoritmo asimétrico para certificar la clave pública, generando un documento electrónico, que lleva la clave pública de un determinado usuario más otra información, todo ello firmado digitalmente por un periodo de tiempo con la privada de la CA que lo emitió.
En una red los servidores pueden ser configurados para permitir el acceso a usuarios con ciertos certificados. Del mismo modo, los clientes pueden ser configurados para confiar en servidores que presentan ciertos certificados.

**-ESTRUCTURA:** La estructura de un certificado viene definida en el estándar ITU X.509 y es el siguiente:




## •FORMATO DE CIFRADO EN PSEUDOCODIGO:

**CIFRAR (CLAVE, <MENSAJE>)**

KPrB= Clave privada de B
KPuA = Clave publica de A
CS = Clave de sesión.
H ["MENSAJE"] = Hash del mensaje. Se utiliza para los resúmenes.

*** EJEMPLO:**

CIFRAR (KPrB, H ["mensaje aleatorio"]) ==> Es la firma digital para un mensaje aleatorio envía por B, al recibir el mensaje.

# 4. Modelos de Seguridad Web:

La seguridad en Internet se puede conseguir de diferentes maneras, podemos establecer seguridad a nivel de red mediante el protocolo IPSec/IPv6. También podemos establecer seguridad en el nivel de transporte, a través de una capa de una capa adicional, transparente a los niveles superiores.
Por último podemos obtener seguridad a nivel de aplicación, este método se utiliza orientándolo a aplicaciones específicas.

## 4.1 Seguridad en el Nivel de Red: IPSec.

IPSec proporciona la capacidad de asegurar las comunicaciones que se efectúen a través de una LAN, a través de una WAN privada o pública y a través de Internet.

La principal característica de IPSec que le permite dar soporte a estas diversas aplicaciones consiste en que puede **CIFRAR Y/O AUTENTICAR TODO EL TRAFICO A NIVEL IP**. Así todas las aplicaciones distribuidas, incluyendo las conexión remota, las aplicaciones cliente/servidor, el correo electrónico, la transferencia de ficheros, el acceso web, etc., pueden hacerse seguras.

IPSec proporciona tres servicios principales: **AUTENTICACION** (AH, cabecera de autenticación), **CONFIDENCIALIDAD** (ESP, encapsulado de carga útil), es una función combinada de autenticación/cifrado y por ultimo una función de **INTERCAMBIO DE CLAVES**, permite el intercambio manual de claves así como un esquema automático.

IPSec tiene dos modos básicos de operación: modo transporte y modo túnel. Estos modos de operación van a usar ESP ya que es más completo que AH.

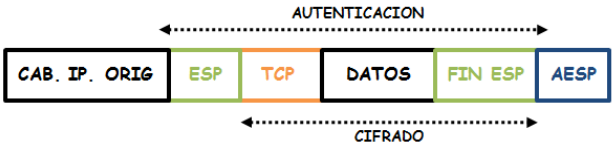
- **MODO TRANSPORTE:**

  Proporciona seguridad extremo a extremo en donde los Computadores de los extremos finales realizan el procesado de seguridad.
  Solo se cifra la carga útil del paquete IP (incluyendo cabecera TCP y de aplicación).
  En el enrutamiento permanece intacto ya que no se modifica, ni se cifra la cabecera IP. Dependiendo del servicio que queramos se añadirá una cabecera u otra:

  **-CONFIDENCIALIDAD:** Se añade la cabecera de encapsulación de carga útil (ESP) que cifra el contenido.


  **-AUTENTICACION:** Cuando se utiliza la cabecera de autenticación (AH) queda autenticado todo el paquete IP excepto los campos mutables, es decir, las direcciones IP.

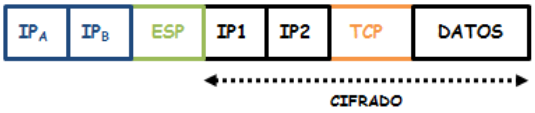

  **-CONFIDENCIALIDAD/AUTENTICACION:** Se añade la cabecera ESP como siempre, pero además se añade en la cola de la cabecera una cabecera adicional, AESP, que autentica el cifrado realizado con la cabecera ESP.



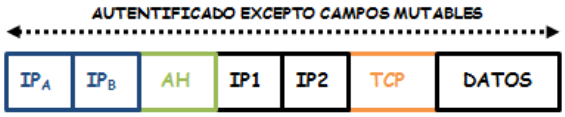

- **MODO TUNEL:**

  La única diferencia es que se cifra todo el paquete IP y luego se encapsula en un nuevo paquete IP, para que funcione el enrutamiento.
  No se puede usar si nos piden seguridad extremo a extremo.

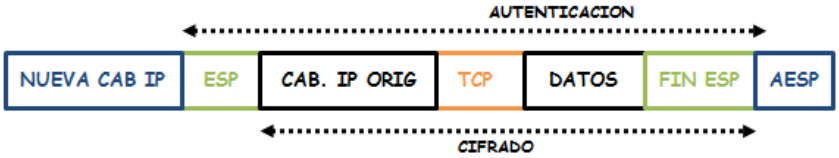
-**CONFIDENCIALIDAD:** Se añade la cabecera de encapsulación de carga útil (ESP) que cifra el contenido.




-**AUTENTICACION:** Cuando se utiliza la cabecera de autenticación (AH) queda autenticado todo el paquete IP excepto los campos mutables, es decir, las direcciones IP.




-**CONFIDENCIALIDAD/AUTENTICACION:** Se añade la cabecera ESP como siempre, pero además se añade en la cola de la cabecera una cabecera adicional, AESP, que autentica el cifrado realizado con la cabecera ESP.



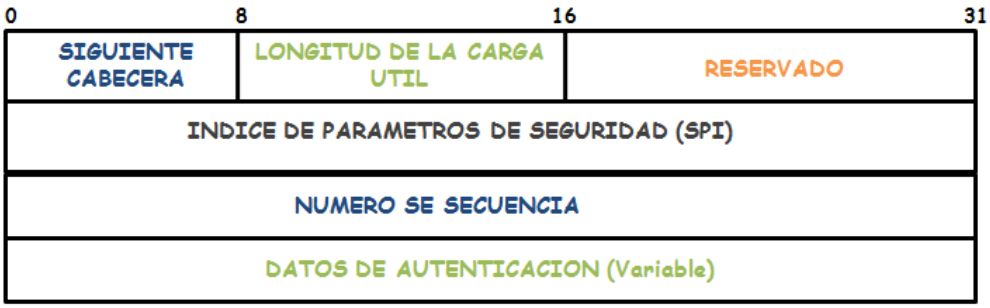

## •FORMATO CABECERA AUTENTICACION IPSEC/IPv6

La cabecera de autenticación proporciona soporte para la integridad de los datos y la autenticación de los paquetes IP. La característica de integridad de los datos segura que sea posible detectar cualquier modificación del contenido de un paquete durante su tránsito.

La característica de la autenticación posibilita a un sistema final o a un dispositivo de red autenticar al usuario o a la aplicación y filtrar el tráfico en consecuencia.

También impide el ataque por falsificación de dirección observado en la actual Internet.

Se basa en el uso de un código de autenticación de mensaje (MAC) y las partes deben compartir la clave secreta.




-**CABECERA SIGUIENTE (8 bits):** Identifica el tipo de cabecera que aparece a continuación.

-**LONGITUD DE CARGA UTIL (8bits):** longitud de la cabecera de autenticación en palabras de 32 bits, menos 2. Por defecto el campo de datos de autenticación es 96 bits (3 palabras), con una cabecera fija de tres palabras, hay un total de seis palabras en la cabecera por lo que el campo longitud de carga útil es de 4.

-**SPI (32 bits):** Índice de parámetros de seguridad, identifica una asociación de seguridad.

-**DATOS DE AUTENTICACION (Variable):** Debe ser un número entero de 32 palabras que contiene el valor de comprobación de integridad, el MAC.

El contenido del campo de datos de autenticación se calcula sobre lo siguiente: Los campos de la cabecera IP que no cambian en el camino o que tienen un valor predecible de AH SA cuando llegue al extremo, la cabecera AH que no sea el campo de datos de autenticación y todos los datos del protocolo de la capa superior, que se suponen inmutables durante el camino.

•FORMATO CABECERA ESP:

Proporciona servicios de privacidad, incluyendo privacidad del contenido de los mensajes y una limitada privacidad del flujo de tráfico. Como una característica opcional puede también proporcionar un servicio de autenticación.


-SPI (32 bits): Índice de parámetros de seguridad, identifica una asociación de seguridad.

-NÚMERO DE SECUENCIA (32 bits): Valor de un contador que se incrementa de forma monótona.

-DATOS DE CARGA UTIL (Variable): Se trata de un segmento de la capa superior protegido mediante cifrado.

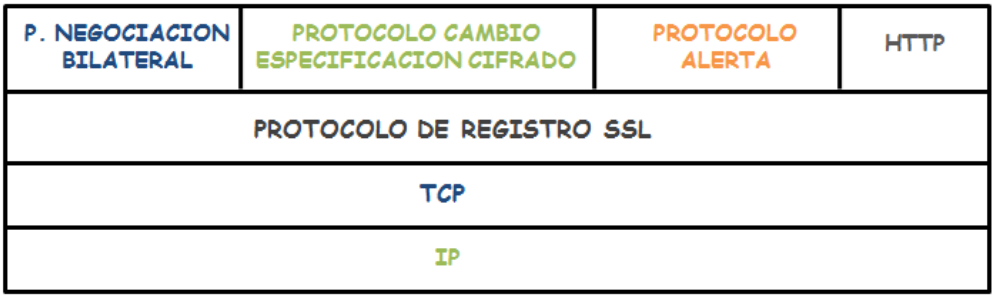
-RELLENO (0-255 octetos): Este campo puede requerirse si el algoritmo de cifrado necesita que el texto nativo sea un múltiplo de algún número de bytes.

-LONGITUD DE RELLENO (8bits): Indica el número de bytes de relleno que preceden inmediatamente a este campo.

-CABECERA SIGUIENTE (8 bits): Identifica el tipo de datos contenidos en el campo de datos de carga útil mediante la identificación de la primera cabecera en esa carga útil.

## 4.2 Seguridad en el Nivel de Transporte

SSL está diseñada para hacer uso de TCP con un objeto de proporcionar un servicio fiable y seguro extremo a extremo. SSL no es el único protocolo sino dos capas de protocolos.




El PROTOCOLO DE REGISTRO de SSL proporciona servicios básicos de seguridad a varios protocolos de capas superiores, en particular, el protocolo http, que proporciona el servicio de transferencia para la interacción entre cliente y servidor web, puede operar sobre SSL.

Tres protocolos de capas superiores se definen como parte de SSL: el PROTOCOLO DE NEGOCIACIÓN BILATERAL SSL, el PROTOCOLO DE CAMBIO DE ESPECIFICACIÓN DEL CIFRADO y el PROTOCOLO DE ALERTA.

Estos protocolos específicos de SSL se utilizan en la gestión de los intercambio SSL.

Dos conceptos importantes de SSL son la Sesión SSL y la Conexión SSL:

-SESIÓN SSL: Una sesión SSL es una asociación entre un cliente y un servidor. Las sesiones las crea el protocolo de negociación bilateral.

Estas definen un conjunto de parámetros de seguridad criptográficos, que pueden compartirse entre múltiples conexiones.

Las sesiones se utilizan para evitar la costosa negociación de nuevos parámetros de seguridad para cada conexión.

-**CONEXIÓN SSL:** Una conexión en un transporte que proporciona un tipo de servicio adecuado. En SSL, dichas conexiones son relaciones entre pares. Las conexiones son transitorias. Cada conexión se asocia con una sesión.

## •PROTOCOLO DE REGISTRO SSL:

Proporciona a las conexiones SSL servicios de **CONFIDENCIAL, e**l protocolo de autenticación define las claves de sesión usadas en el cifrado/descifrado y de **INTEGRIDAD DEL MENSAJE,** el protocolo de autenticación define la clave secreta utilizada en un código de autenticación de mensajes (MAC).

**-FUNCIONAMIENTO:**

* **FRAGMENTACION:** Se fragmenta cada mensaje de la capa superior en bloques de cómo máximo $2^{14}$ bytes
* **COMPRESION:** Opcional.
* **AÑADIR MAC:** Se calcula un código de autenticación de mensaje sobre los datos comprimidos, después el mensaje comprimido más el MAC son cifrados utilizando un cifrado simétrico.
* **FRAGMENTACION:** Se fragmenta cada mensaje de la capa superior en bloques de cómo máximo $2^{14}$ bytes
* **INSERCION CABECERA DE REGISTRO SSL**

El protocolo de registro transmite después la unidad resultante en un segmento TCP. Los datos recibidos se descifran, verifican, descomprimen y reensamblan y entonces se entregan al usuario.

## •PROTOCOLO DE CAMBIO DE ESPECIFICACION DE CIFRADO:

El protocolo de cambio de especificación de cifrado es uno de los tres protocolos específicos de SSL que usa el protocolo de registro SSL, siendo el más simple.

Este protocolo consta de un solo mensaje, que consiste en un solo byte con el valor 1. El único propósito de este mensaje es provocar que se copie el estado pendiente en el estado actual, lo que actualiza el repertorio de cifrado a utilizar en esta conexión.

## •PROTOCOLO DE ALERTA:

El protocolo de alerta se usa para transportar las alertas relacionadas con SSL a la entidad par. Los mensajes de alerta se comprimen y cifran, según lo especificado en el estado actual.

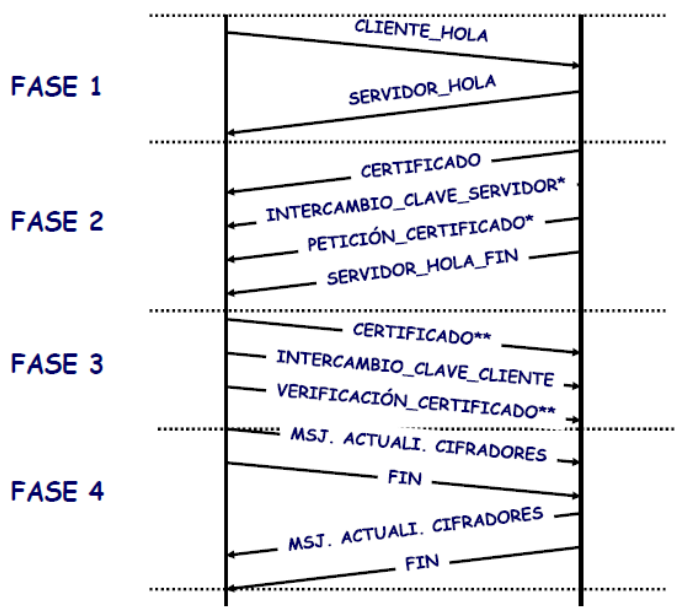
Cada mensaje de este protocolo consta de dos bytes. El primer byte se usa para transmitir la gravedad del mensaje. El segundo byte contiene un código que describe la alerta concreta.

## •PROTOCOLO DE NEGACIACION BILATERAL:

Este protocolo permite al servidor y al cliente autenticarse mutuamente para negociar unos algoritmos de cifrado y de MAC y las claves criptográficas que se usaran para proteger los datos enviados en los registros SSL.

Se utiliza antes de que se transmita ningún dato de aplicación.

El protocolo de negociación bilateral consta de una serie de mensajes que se intercambian el cliente y el servidor:



**-FASE 1: ESTABLECIMIENTO DE PARAMETROS DE COMUNICACIÓN.**

Se utiliza para iniciar una conexión lógica y establecer las capacidades de seguridad que se le asociarán. El intercambio lo inicia el cliente el cual envía un mensaje **"SALUDO DE CLIENTE".**

El contenido del mensaje es, versión de protocolo, identificador de sesión, repertorio de cifrado, método de compresión y números aleatorios iniciales.

Tras enviar el "SALUDO DE CLIENTE", el cliente espera el mensaje "SALUDO DE SERVIDOR" que contiene los mismos parámetros.

**-FASE 2: AUTENTICACION DEL SERVIDOR.**

Depende del esquema de cifrado de clave pública subyacente utilizada. En algunos casos, el servidor pasa un certificado al cliente, posible información adicional de la clave y una solicitud del certificado del cliente.

En general el servidor envía: **CERTIFICADO** de clave publica, **INTERCAMBIAR LAS CLAVES**, el servidor puede crear un par de claves publica/privada y envía al clienta un certificado de clave publica y **SOLICITAR CERTIFICADO**, el servido puede pedir un certificado al cliente, el mensaje incluye el tipo de certificado y una lista de autoridades de certificación aceptables..

El servidor es el que indica el fin de la fase. **("FIN SALUDO DE SERVIDOR"),** el cual es obligatorio.

**-FASE 3: AUTENTICACION DEL CLIENTE E INTERCAMBIO DE CLAVE DE SESION.**

Al recibir el mensaje "FIN SALUDO SERVIDOR", el cliente debe verificar que el servidor proporciono un certificado valido, si es necesario, y verificar que los parámetros del mensaje "SALUDO SERVIDOR" se aceptan.

Si todo es satisfactorio, el cliente envía uno o más mensajes de vuelta al servidor, dependiendo del mensaje de clave publica.

Los más habituales son: **CERTIFICADO**, solo es obligatorio si lo ha solicitado el servidor, **INTERCAMBIO CLAVE CLIENTE**, el cliente genera una pre-master secret de 48 bytes cifrada con clave publica del servidor, que se utilizara para generar las claves de sesión y las claves MAC tanto por el servidor como por el cliente. El mensaje de **VERIFICACION DE CERTIFICADO** se envía solo si se ha solicitado por el servidor, se envía junto con el mensaje anterior. Consta de una firma Hash y el cifrado se hace con clave privada del cliente.

**-FASE 4: FASE FINAL.**

Completa el establecimiento de una conexión segura. El cliente envía un mensaje **"CAMBIO DE ESPECIFICACION DE CIFRADO"** y copia la especificación de cifrado pendiente sobre la especificación de cifrado actual.

Inmediatamente el cliente envía el mensaje de **"FINALIZADO"** bajo los nuevos algoritmos, claves y secretos. El mensaje "FINALIZADO" verifica que los procesos de intercambio de clave y autenticación fueron satisfactorios.

En respuesta a eso dos mensajes el servido repite el mismo procedimiento que el cliente.

En este punto, la negociación bilateral esta completa y el cliente y el servidor pueden empezar a intercambiar datos de la capa de aplicación.